CHAPTER

# 9

# REMOTE ACCESS SERVICE

**After reading this chapter and completing the exercises, you will be able to:**

- Understand remote access under Windows 2000
- Configure various RAS connection types for a Windows 2000 Professional system
- Enable offline file access
- Troubleshoot RAS problems

When it comes to network access, not all access occurs from computers that are directly attached to the network where the resources and data reside. Especially for roving workers, such as salespeople and field engineers, and increasingly for telecommuters as well, the ability to gain access to a network remotely—that is, from some location other than where the network itself resides—is an important capability. This is an area where Windows 2000 really shines: it is one of the few major network operating systems that includes remote access capabilities with the core software at no additional charge. For Windows 2000 Professional, this means that a single dial-in or dial-out connection that can use a modem, an **ISDN (Integrated Services Digital Network)** line, frame relay, or any of the other, more exotic digital remote link technologies is part of the package. For Windows 2000 Server, a complete multiuser Remote Access Server is included with the core offering, and it can support up to 256 simultaneous dial-in/dial-out connections. Since Windows NT 3.51 became a force to be reckoned with in 1995, remote access services have played a crucial role in its burgeoning popularity and widespread acceptance through the current Windows 2000 release.

## REMOTE ACCESS SERVICE (RAS)

You can use the **Remote Access Service (RAS)** to log on to a Windows 2000 system for user or administrative access while you are away from the office. For example, when you are traveling on business, you can access the system from a hotel room.


RAS initiates and maintains the access information from the client system. A client system is defined as a Windows 2000, Windows NT, or Windows 95/98 system that initiates access to a Windows 2000 system established as a remote access server.

A Windows 2000 RAS configuration includes the following components:

- *Clients:* Windows 2000, Windows NT, Windows 95/98, Windows for Workgroups, MS-DOS (with Microsoft network client software installed), and LAN Manager RAS clients can all connect to a Windows 2000 RAS server. Clients can also be any platform that supports the **Point-to-Point Protocol (PPP)**. PPP provides connectivity over serial or modem lines, and can negotiate any transport protocol used by both systems involved in the link.
- *Protocols:* Windows 2000 RAS servers support the PPP protocol, enabling any PPP client to use the Transmission Control Protocol/Internet Protocol (TCP/IP), NWLink (IPX/SPX), or NetBEUI. Windows 2000 as a dial-up client can also access the installed base of **Serial Line Internet Protocol (SLIP)** remote access servers. SLIP is an implementation of the IP protocol over serial lines; however, SLIP cannot be used to connect to a Windows 2000 RAS system. Windows 2000 RAS can accept inbound calls from AppleTalk clients using AppleTalk Remote Access Protocol (ARAP). Windows 2000 RAS also includes backward-compatible support for the RAS protocol (a.k.a. Asynchronous NetBEUI or AsyBEUI) used by legacy clients, such as Windows NT 3.1, Windows for Workgroups, MS-DOS, and LAN Manager.
- *WAN connectivity:* Clients can dial in using standard telephone lines with a modem or modem pool, employing legacy analog or the new Asymmetric Digital Subscriber Line (ADSL) technology. Faster links are possible using ISDN or T-carrier lines. You can also connect RAS clients to RAS servers by using X.25, Asynchonous Transfer Mode (ATM, discussed in Chapter 7), or an RS-232C null modem. Windows 2000 also supports **Multilink PPP**, which is the ability of RAS to aggregate multiple data streams into one network connection for the purpose of using more than one modem or ISDN channel in a single connection. Windows 2000 also supports cable modems; however, in most cases, proprietary software and drivers from the vendor are used to establish connections over these network adapter-like devices because they don't function quite like a modem.
- *Security:* Windows 2000 logon and domain security, support for security hosts, data encryption, and callback provide secure network access for remote clients. With Windows 2000, you also have the option of separating LAN traffic from RAS traffic with the **Point-to-Point Tunneling Protocol (PPTP)** or the **Layer 2**

**Tunneling Protocol (L2TP)**. PPTP allows users to create secure connections to corporate networks over the Internet, using **virtual private networks (VPNs)**, which are network connections that use encryption to transport private data across public links. L2TP is a VPN protocol developed by Cisco to improve security over Internet links by integrating **IPSec (IP Security)**.

- *Server:* Windows 2000 Server RAS allows up to 256 remote clients to dial in. Windows 2000 Professional allows one remote client to dial in. The RAS server can be configured to provide access to an entire network or to limit access to the RAS server only.
- *LAN protocols:* IP protocol support allows you to access a TCP/IP network, such as the Internet. NWLink (IPX/SPX) protocol support enables remote clients to access NetWare servers and printers. You can also use NetBIOS applications over IPX, TCP/IP, or NetBEUI. Windows Sockets applications over TCP/IP or IPX, named pipes, Remote Procedure Call (RPC), and the LAN Manager API are also supported (see Chapter 7).


Remote control and RAS are two remote technologies that work in different ways. Remote control employs a remote client as a dumb terminal for the answering system, whereas RAS establishes an actual network connection between a remote client and the answering computer system, using a link device (such as a modem) as a network adapter. RAS keyboard entries and mouse movements occur locally; with remote control, these actions are passed to a host system. Using RAS, computing operations are executed on the client; remote control computing operations are executed on the host with the resultant video signal being sent to the client.



Remote access services and terminal services are also two different mechanisms. Terminal services allow thin clients (that is, basic computers consisting of a display, keyboard, and mouse with only enough intelligence to connect to the terminal server host) to participate in a rich computing environment. Basically, the terminal server host acts as the CPU for the thin client. All operations and calculations are performed on the terminal server host; only the display changes are sent to the client, and only keyboard and mouse information is sent back to the terminal server. Terminal services are often employed in situations in which budget restrictions prevent the purchase of fully capable desktop systems or when complete security is required (that is, not allowing data to exist anywhere but on the secure server). RAS, on the other hand, is a mechanism by which remote computers that exist as independent systems are able to make connections over some type of communications link to a system or standalone machine. This link is used to access data or to gain further access to linked networks.

## Features of RAS in Windows 2000

RAS is an integral part of Windows 2000. In fact, RAS is a standard component of Windows 2000 and does not require a manual installation to enable remote access, as was required in Windows NT. Some of the impressive features of RAS under Windows 2000 include: Multilink PPP, PPTP, L2TP, restartable file copy, idle disconnect, autodial and logon

dial, client and server enhancements, a new look and feel, and callback security, each of which is defined as follows:

- *Multilink PPP RAS:* Multilink PPP allows you to increase overall throughput by combining the bandwidth of two or more physical communications links, such as analog modems, ISDN, and other analog/digital links.
- *Point-to-Point Tunneling Protocol (PPTP):* PPTP is a networking technology that supports multiprotocol VPNs, which allow users to access corporate networks securely via the Internet. Using PPTP, you can shift the burden of hardware support for devices such as modems and ISDN cards from the RAS server to a front-end processor (FEP) located at the Internet service provider (ISP). Clients using PPTP can access a corporate LAN by dialing an ISP or directly through the Internet. In both cases, the PPTP tunnel is encrypted and secure, and works with any protocol.
- *Layer 2 Tunneling Protocol (L2TP):* The Layer 2 Tunneling Protocol (L2TP) is a PPTP alternative that has been developed by Cisco Systems. Similar to PPTP, L2TP encapsulates PPP frames for transport over various networks, including IP, X.25, frame relay, and ATM. L2TP is used in combination with IPSec (a security protocol that secures data at the packet level) to provide a secure encrypted VPN link over public networks.
- ***Restartable file copy:*** The restartable file copy feature automatically retransmits file transfers that are incomplete because of RAS connectivity interruption. This feature reduces the time it takes to transmit large files over lower-quality connections, cost (because it avoids retransmission of the whole file), and the frustration that accompanies interrupted transfers.
- ***Idle disconnect:*** The idle disconnect feature breaks off a RAS connection after a specified period of time has gone by with no activity. This feature reduces the costs of remote access, helps you troubleshoot by closing dead connections, and frees up inactive RAS **ports** (any physical communication channel to which a modem, direct cable, or other device can be connected to enable a link between two computers).
- *Autodial and Logon Dial:* You can configure RAS access to automatically connect and retrieve files and applications stored on a remote system. Users do not have to establish an RAS connection each time they want to transfer a remote object; Windows 2000 handles all RAS events, providing quick and efficient access. By maintaining a virtual database of mappings between resources and connection objects, Windows 2000 RAS is able to reestablish links when previously accessed resources are requested.
- *Client and server enhancements:* Windows 2000 RAS includes a number of client and server components that allow third-party vendors to develop RAS and dial-up networking applications.
- *Look and feel*: Windows 2000 RAS is somewhat different from its manifestations in Windows NT or even Windows 95/98. The RAS capabilities have been integrated

with the networking components, which results in a multipurpose management interface in which both standard LAN networking links and RAS links are established and configured. The Network and Dial-up Connections interface is a new, centralized control mechanism. Just about everything related to RAS is controlled through this interface. The only exception is that all RAS hardware, such as a modem, is installed through the Add/Remove Hardware applet in the Control Panel.

- *Callback security:* You can control access to the system from specified phone numbers by using callback security. Selecting the Call Back radio button forces calls to originate from known phone numbers ("Preset to" option), or the remote access client can set the phone number dynamically ("Set by Caller" option). Setting the number dynamically allows users to access the system from different phone numbers even with the callback feature enabled and negates the callback security feature because remote access can be accomplished from any phone number.

## WAN Connectivity



Wide area networks (WANs) link sites that are often a considerable distance apart. Using RAS and Windows 2000 enables you to create a WAN by connecting existing LANs via RAS over telephone, ISDN, or other communications lines. This is an inexpensive and cost-effective solution if you have minimal-to-moderate network traffic between sites. You can improve the performance of RAS-based WANs in one of three ways:

- Increase the RAS connection bandwidth
- Link multiple communication links, using Multilink PPP
- Implement PPTP over the Internet

## Internet Network Access Protocols

Windows 2000 RAS supports all standard protocols for remote Internet access as well as Multilink PPP. The RAS protocol that is used to establish and maintain a WAN link is dependent on the client and server operating system and the LAN protocols. Windows-2000-supported RAS protocols are discussed in the following sections.

### Point-to-Point Protocol (PPP)

PPP is the current remote access standard. Remote access protocol standards are defined in RFCs (Request for Comments), official standards documents published by the Internet Engineering Task Force (IETF). You can find detailed information on the following RFCs at *http://www.ietf.org/rfc*. The RFCs supported in Windows 2000 RAS are:

- RFC 1661: The Point-to-Point Protocol (PPP)
- RFC 1549: PPP in HDLC Framing

- RFC 1552: The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
- RFC 1334: PPP Authentication Protocols
- RFC 1332: The PPP Internet Protocol Control Protocol (IPCP)

Microsoft recommends using PPP because it is flexible and an industry standard, which means continued compatibility with client and server hardware and software in the future. Remote clients connecting to third-party PPP servers may need to use a post-connect terminal script (a script that provides login information to log on to the PPP server). The server will inform users it is switching to PPP framing mode (users must start the terminal to complete logon).


When using a version of PPP other than Microsoft's to dial into a Windows 2000 Server that is a part of a domain and not a domain controller, the server looks only to its local accounts for the account name and password you specified on dial-in. If the server doesn't find the name and password locally, it doesn't check the domain accounts; it simply denies access. A domain controller does not have local accounts that it can use for verification; it uses the accounts in the domain database to grant or deny access.

## Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) is one of the most interesting features of Windows 2000: it allows you to establish a secure RAS pipeline over the public Internet and to "tunnel" IPX, NetBEUI, or TCP/IP traffic inside PPP packets. PPTP can provide real benefits for companies with numerous remote users who already subscribe to a local ISP for e-mail and Internet access, because they can use the same connection to access the corporate LAN. These VPNs can support the IPX, TCP/IP, and NetBEUI LAN protocols and provide private network access from any Internet connection point. PPTP's significant features include:

- *Reduced transmission costs:* PPTP uses the Internet as the primary long-distance connection medium rather than leased lines or long-distance telephone lines, which reduces the cost of establishing and maintaining a RAS connection.
- *Reduced hardware costs:* PPTP requires less hardware by letting you locate modems and ISDN hardware on a network rather than directly attaching them to the RAS server.
- *Less administrative overhead*: PPTP permits centralized management of RAS networks and users.
- *Improved security:* PPTP connections over the Internet are encrypted and secure.

L2TP is a protocol similar to PPTP developed by Cisco for use with IPSec to support secure VPN links. From a user's perspective, it operates in the same manner as PPTP.

## Multilink PPP

Multilink PPP combines two or more physical RAS links (modem, ISDN, or X.25 links) into one logical bundle with greater bandwidth. Multilink can combine analog and digital links in the same logical bundle. The only drawback to Multilink is that all connections to be aggregated must be of the same technology type. For example, ISDN and modem links cannot be aggregated, but three ISDN lines can be.

Because only one phone number can be stored in a user account, Multilink will not function with the callback security feature. The only exception to this rule is dual ISDN lines that have the same phone number. In this one instance, callback security will work with multilink.

## Microsoft RAS Protocol (Asynchronous NetBEUI)

Microsoft's proprietary RAS protocol supports NetBEUI; any RAS client dialing into a Windows NT 3.1 or Windows for Workgroups system must use this protocol. When a connection has been established, the RAS server will act as a **gateway** for the remote client, providing access to resources via the NetBEUI, TCP/IP, or IPX protocols.



## NetBIOS Gateway

Microsoft includes the **NetBIOS gateway** in Windows 2000 to enable backward compatibility for earlier versions of Windows NT, Windows for Workgroups, and LAN Manager. Remote clients connect using NetBEUI, and the RAS server translates packets as necessary between clients and local IPX or TCP/IP resources and servers. The NetBIOS gateway allows client access to LAN resources without local support for IPX or TCP/IP.

## Serial Line Internet Protocol (SLIP)

SLIP was one of the first protocols developed specifically for TCP/IP support over dial-up connections. SLIP is not used much anymore because of its limitations as compared to PPP. For example, SLIP does not support the **Dynamic Host Configuration Protocol (DHCP)**, a method of dynamically assigning IP addresses, so a static IP address must be assigned to every SLIP client, which makes IP address administration more difficult. Unlike PPP, SLIP does not support IPX or NetBEUI. However, SLIP's biggest drawback is that it does not support encrypted passwords; its passwords are transmitted as plain text. RAS does not offer a SLIP server. RAS supports SLIP only as a client, which allows Windows 2000 clients to access UNIX servers that support SLIP.

The RFCs supported by RAS SLIP are:

- RFC 1144: Compressing TCP/IP Headers for Low-Speed Serial Links
- RFC 1055: A Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP

## Telephony Features of RAS

The RAS **Telephony Application Programming Interface (TAPI)** supplies a uniform way of accessing fax, data, and voice. TAPI is part of the Windows Open System Architecture (WOSA), developed to aid third-party vendors in designing powerful, integrated telephony applications. TAPI handles all communication between a TAPI-aware computer and a Private Branch Exchange (PBX), including basic phone functions (call park, hold, transfer, conferencing, and so on). TAPI treats a telephone network as a system resource using standard APIs and device drivers, so once installed, TAPI applications have seamless access to phone features and server-based communications.

Here are some of the benefits of and improvements in TAPI 3.0:

- *Comprehensive support:* TAPI is packaged with Windows 95, Windows 98, and Windows NT 4.0 Server and Workstation, as well as with Windows 2000 Server and Professional.
- *Native 32-bit components:* TAPI 3.0 core components are 32-bit and have additional full support for symmetrical multiprocessing, multithreaded applications, and preemptive multitasking.
- *Portability:* 32-bit TAPI applications designed for one TAPI platform will run without modification on any other, including Windows 95, Windows 98, Windows NT, and Windows 2000.
- *Device sharing capability:* Separate applications for inbound and outbound calls can control a single device, reducing hardware costs and enlarging the communications capacities of small business.

For more information about TAPI 3.0, refer to the IP Telephony with TAPI 3.0 white paper at *http://www.microsoft.com/windows/server/Technical/networking/iptelephony.asp*.

## Configuration of RAS

Unlike Windows NT, RAS under Windows 2000 is an integrated default component of the operating system. Therefore, no additional service installation is required to take immediate advantage of the communication offered via RAS. RAS is configured and managed from the Network and Dial-up Connections window (see Figure 9-1). (Dial-up connections were discussed in Chapter 7.) This window is accessed by selecting Start, Settings, Network and Dial-up Connections.

You have to create all RAS or remote links. The Make New Connection Wizard is used to establish new connections. You launch this wizard by double-clicking the Make New Connection icon in the Network and Dial-up Connections window. Five remote connection options are offered to you, as you can see in the Network Connection Type window shown in Figure 9-2.

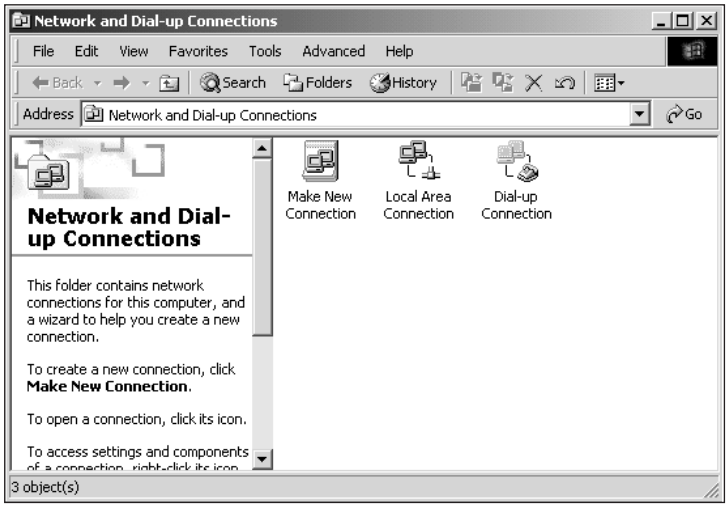


**Figure 9-1** The Network and Dial-up Connections window



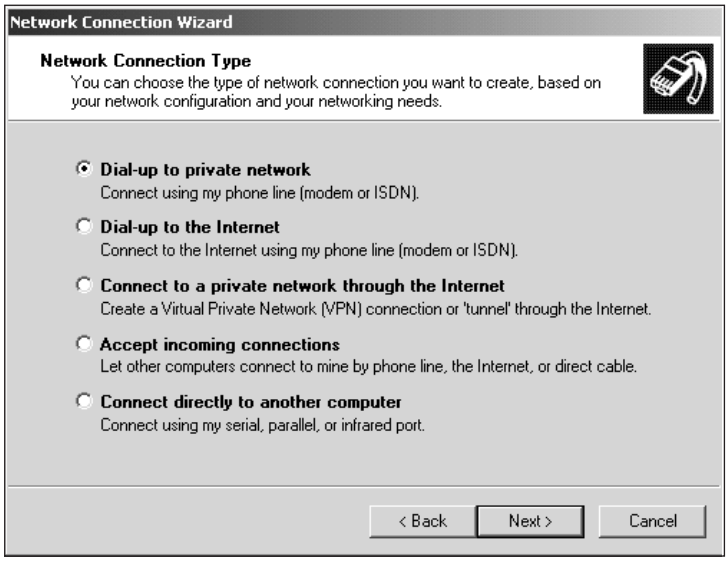


**Figure 9-2** The select network connection type page of the Make New Connection Wizard

The options are as follows:

- *Dial-up to private network:* This option is used to create a connection object used to establish communications with a Windows 2000 or Windows NT RAS server.
- *Dial-up to the Internet:* This option is used to create a connection object used to establish communications with an ISP to gain Internet access.

- *Connect to a private network through the Internet:* This option is used to create a connection object used to establish a VPN connection to a remote LAN over a public network (such as the Internet). This connection can employ either PPTP or L2TP.
- *Accept incoming connections:* This option configures the system to accept inbound calls or connections. Windows 2000 Professional can only support a single inbound connection, but that link can be a direct connection, modem/dial-up connection, or a VPN link.
- *Connect directly to another computer:* This option is used to create a connection object used to establish communications over a serial cable, parallel cable, or infrared port.

Establishing RAS connection objects via the wizard is very elegant and quick. In the following sections, you look at the step-by-step process for each of these connection types and the postcreation properties you can manipulate.

All of the following network connection types require that the hardware device used to establish the RAS link be installed and configured before creating the connection object. This includes modems, cable modems, ADSL devices, infrared ports, and so on. See the section titled "Installing RAS Hardware" later in this chapter for information on device installation.

## Dial-up to Private Network

Telecommuters and mobile personnel often need to communicate with the office LAN for a wide variety of purposes. Because a RAS link supports all network functions, such as access to files, printers, the Internet, various network services, and security control, remote connections to the LAN are very useful. Many organizations are taking advantage of the distance communication enabled by Windows 2000, Windows NT, and Windows 95/98 to reduce office space costs and increase the productivity of their employees. You can establish telecommuting with ease. The Dial-up to private network connection type is used for all connections over temporary communications lines between a remote client and a RAS server. To create a connection object on a remote client to be used to connect to a RAS server, follow the steps described in Hands-on Project 9-1.

After a Dial-Up to Private Network connection object is created, the Connect dialog box is automatically launched. The Connect dialog box offers four action buttons at the bottom of its display (see Figure 9-3). The Dial button launches the connection and attempts to establish a connection using the defined settings. The Cancel button closes the Connect dialog box and discards any changes made to that dialog box. The Properties button opens the multitabbed Properties dialog box for the connection object. The Help button launches the Windows 2000 Help system in the Network and Dial-up Connections context section.

In most cases, you want to click Dial to test the new object. If the connection is successful, an icon appears in the icon tray of the taskbar. The icon looks like two overlapping monitors. Each time a packet is passed over the connection, the color of the monitor screen flashes and changes from gray to teal. Double-clicking this icon reveals a connection status page, which can be used to access the connection's properties or to disconnect the link. You can also right-click over the tray icon to access dial-up properties or disconnect functions.

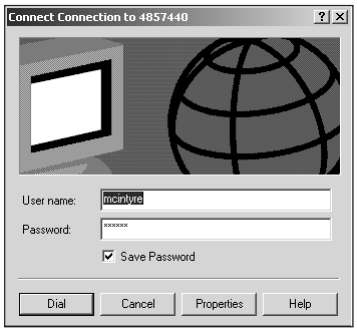


**Figure 9-3** The Connect dialog box

A private network connection object functions by using the default settings in most cases, but you may want to fine-tune your connection to improve performance or capabilities. The Properties dialog box for a connection object can be accessed through a variety of means:

- Select the connection object in the Network and Dial-up Connections window, then either select Properties from the File menu or right-click the icon and select Properties from the resulting menu.
- If the connection object is already in use, right-click the tray icon and select Properties from the resulting menu.
- If the connection object is already in use, double-click the tray icon, then click the Properties button in the Status dialog box.

No matter how you get there, the Properties dialog box (shown in Figure 9-4) for a private network connection object is used to configure a wide variety of settings that are not offered via the Make New Connection Wizard.

The General tab is used to configure the devices and dial-up numbers. The "Connect using" field lists all installed communications devices. The devices with a marked check box are employed by the connection object in an attempt to establish a connection. The listed devices can be ordered to give priority to the faster or more reliable devices. By default, all devices dial the same phone number. If you deselect the "All devices call the same number" check box, the Phone number area becomes dependent on the selection of a device. The Phone number area includes settings for the area code, phone number, country/region code, and dialing rules. (See the "Phone and Modem Options" section later in this chapter for more information.) You can configure individual devices by clicking the Configure button when a device is selected. This opens a device-specific configuration dialog box in which elements such as communication speed, modem protocols, hardware features, terminal window, logon scripts, and modem speaker are configured. Note that settings in this dialog box apply only to the selected device. The Options tab includes connection object settings for the terminal window and logon scripts. The "Show icon in taskbar when connected" check box enables an icon for this connection to appear in the icon tray. This icon is used for quick access to connected links.

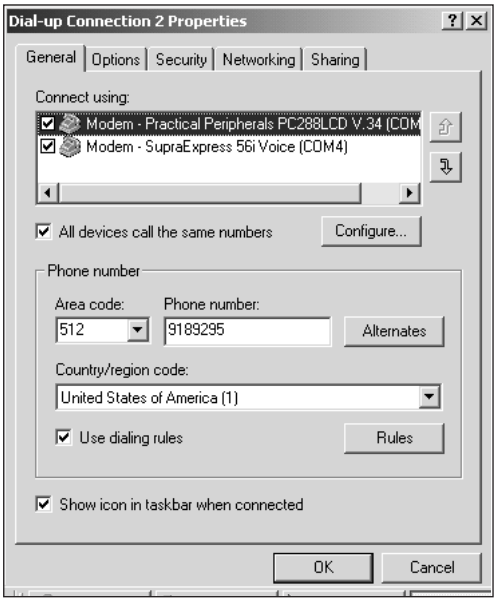


**Figure 9-4** The Properties dialog box for a private network connection object, General tab

The Options tab (see Figure 9-5) configures how the connection object behaves while establishing a connection.

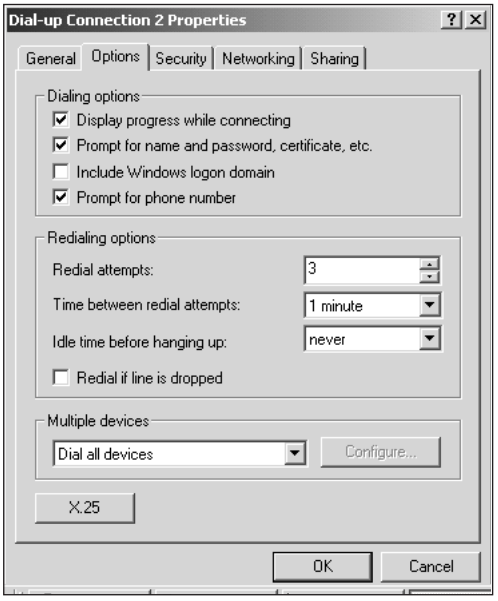


**Figure 9-5** The Properties dialog box for a private network connection object, Options tab

The available settings on the Options tab are:

- *Display progress while connecting*—Provides you with a visual status of the connection establishment process. This option is selected by default.
- *Prompt for name and password, certificate, etc.*—Forces you to provide access credentials before launching the Connection object. This option is selected by default.
- *Include Windows logon domain*—Forces the connection to request logon domain information from the RAS server. By default, this option is not selected.
- *Prompt for phone number*—Forces the connection object to always prompt for verification of the phone number before attempting to establish a connection. This option is selected by default.
- *Redial attempts*—Sets the number of retries the system will make when a connection cannot be established with the remote system. The default is three retries.
- *Time between redial attempts*—Sets the time period between redials. The default is 1 minute.
- *Idle time before hanging up*—Sets the inactivity disconnect time period. The default is never.
- *Redial if line is dropped*—Forces the connection object to attempt to reconnect if the link is broken for any reason.
- *Multiple devices*—Used to enable Multilink. This is set to "Dial all devices" by default. Other settings include "Dial only first available device," which only establishes a single link with the remote system, and "Dial devices only as needed," which is used to establish activity-based dialing. Clicking the Configure button for the latter selection opens the Automatic Dialing And Hanging Up dialog box (see Figure 9-6). This dialog box is used to define when additional devices are dialed or disconnected, based on the level and time period of traffic. Defaults are to dial using new devices when current bandwidth has been at 75% utilization for 2 minutes and to disconnect when utilization has been less than 10% for 2 minutes.
- *The X.25 button*—Opens the configuration dialog box for X.25 connections. Through this dialog box you can define the X.25 network type in use, your X.25 address, and the two optional settings of user data and facilities. For more information on X.25, consult the *Windows 2000 Resource Kit*.

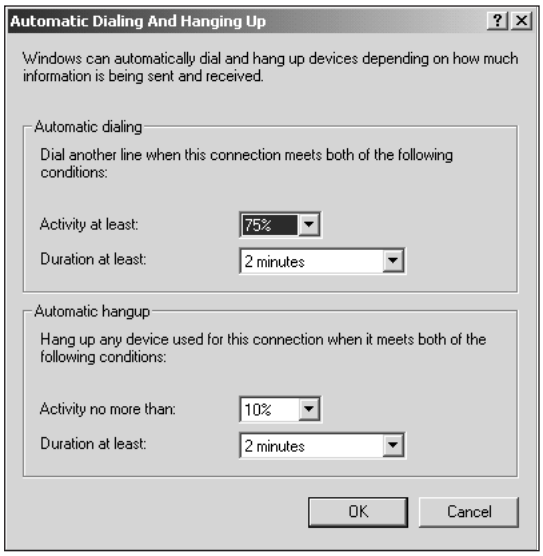


**Figure 9-6** Automatic Dialing and Hanging Up dialog box

The Security tab (see Figure 9-7) is used to define the security requirements of the connection object. This tab offers two top-level security settings: "Typical (recommended settings)" and "Advanced (custom settings)." The default setting is "Typical (recommended settings)," which allows for unsecured passwords and has two other options: Require secured password and Use smart card. Two check boxes further define these alternate security options. The "Automatically use my Windows logon name and password (and domain if any)" check box should be used when your local and remote logon credentials are identical. The "Require data encryption (disconnect if none)" option protects not only the authentication process, but also all data transferred over the link.

The second top-level security setting of "Advanced (custom settings)" is used to specify exactly the level of security to use for this connection object. The Settings button reveals the Advanced Security Settings dialog box (see Figure 9-8).

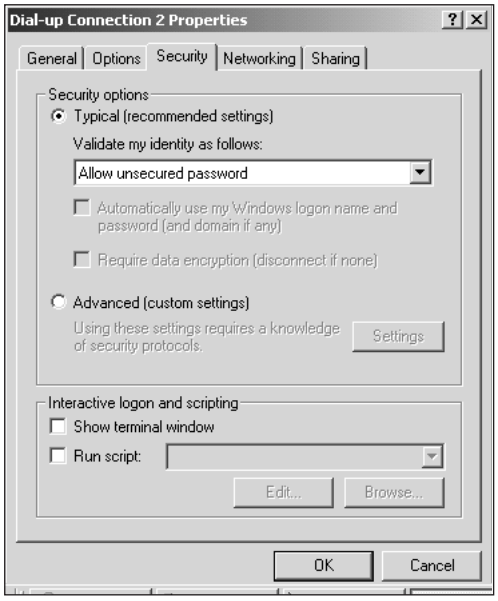


**Figure 9-7** The Properties dialog box for a private network connection object, Security tab

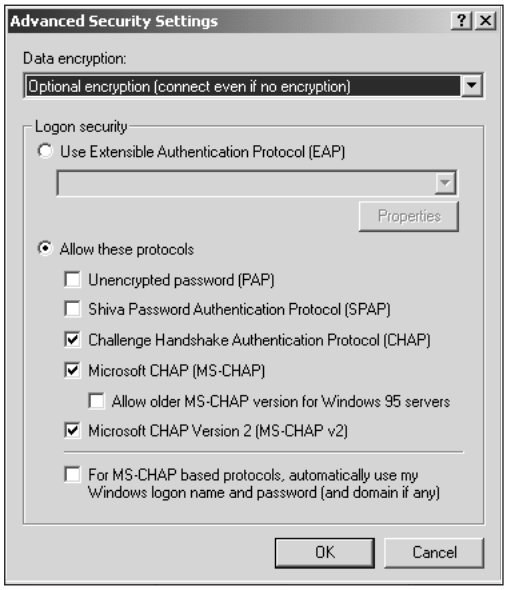


**Figure 9-8** Advanced Security Settings dialog box

The Advanced Security Settings dialog box offers the following settings:

- *Data encryption*—Defines the encryption requirements. Selections are "No encryption allowed (server will disconnect if it requires encryption)," "Optional encryption (connect even if no encryption)," and "Require encryption (disconnect if server declines)."
- *Use Extensible Authentication Protocol (EAP)*—Allows you to require the use of smart card or third-party security mechanisms. The Properties button accesses mechanism-specific configuration settings.
- *Allow these protocols*—Select the encryption protocols allowed over this connection object. Options include the Password Authentication Protocol (PAP), the Shiva Password Authentication Protocol (SPAP), the Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), MS-CHAP for Windows 95 servers, and MS-CHAP v2.
- *Use Windows logon name and password (and domain if any) automatically for MS-CHAP based protocols*—Uses local logon credentials over the connection object.


Defining custom security settings can be a complex and intricate process. We recommend consulting the *Windows 2000 Resource Kit* for more information on custom security settings before you attempt to deploy a custom security scheme on your network or over your RAS connections.

The bottom of the Security tab offers controls over whether to pop up a terminal window and run a script after a connection is established. These settings apply to all devices used by this connection object. To define device-specific items, use the Configure button on the General tab. In most cases, terminal windows and logon scripts are unnecessary; however, depending on the type of server you are connecting to and the security mechanisms employed, you may need to alter these settings. A terminal window allows you to enter keystrokes directly into the authentication mechanism on the remote server. Some systems require multiple passwords, selecting a logon method from a menu, or issuing protocol launch commands. If the logon requirements of a system can be automated, you can create a logon script that will provide these items automatically, without requiring a terminal window and user input each time the connection is established. Dial-up logon scripts can be as complex as necessary, and can include branching decision trees based on data from the remote server. Windows 2000 includes several sample scripts in the %systemroot%\System32\RAS folder that you can customize for your own purposes. For details on creating and modifying logon scripts, please consult the content of the sample scripts (which include useful details in the form of context-specific comments) and the *Windows 2000 Resource Kit*.

The Networking tab (see Figure 9-9) is used to configure the network communication components employed by the connection object. As you can see, this tab is very similar to the Properties window of a local area connection object. Keep in mind that a RAS connection is the same as a local connection, with a difference only in the speed of the connection, so this similarity should not surprise you.

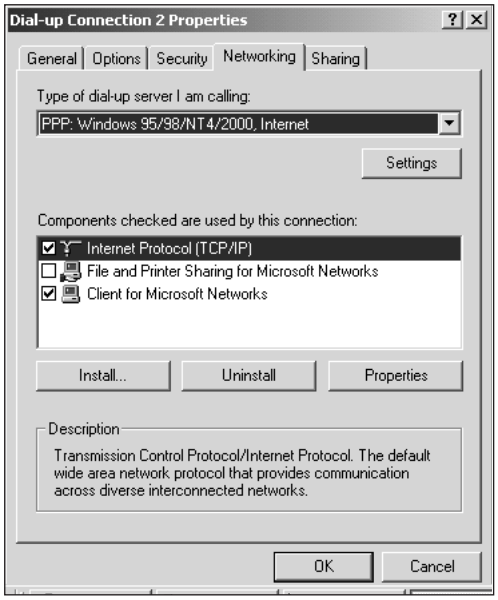


**Figure 9-9** The Properties dialog box for a private network connection object, Networking tab

The most important setting on this tab is the type of dial-up server to which this connection object is to connect. Your options are PPP and SLIP. Because Windows 2000 and Windows NT RAS servers can only accept inbound PPP connections, you will most likely select PPP; however, if you are connecting to an older UNIX system, you may need to employ SLIP. If you don't know which to choose, try PPP first because it is the current standard remote link connection technology. PPP offers two further configuration details via the Settings button: enabling Link Control Protocol (LCP) extensions and enabling software compression. In most cases, the default settings are correct, but when connecting to older UNIX (or other) platforms, the LCP extensions and software compression capabilities of the Windows 2000 version of PPP may prevent stable communications.

The remaining portion of this tab is used to enable, install, and configure networking components. Enabling and disabling a component applies only to this connection object, but installing or removing a component applies to all connection objects. By default, only the Internet Protocol (TCP/IP) and Client for Microsoft Networks components are enabled; the File and Print Sharing for Microsoft Networks component is disabled. For information on configuring network components, refer to Chapter 7.

The Sharing tab (see Figure 9-10) is used to configure this connection object as a shared communications channel. By enabling sharing for a connection object, you allow other computers on your network to access resources over that external link. This feature, known as Internet Connection Sharing, can be employed for either standard LAN or Internet connections. Internet Connection Sharing incorporates the Network Address Translation (NAT) function, a Dynamic Host Configuration Protocol (DHCP) address allocator, and a Domain

Name Service (DNS) proxy. The mechanism hides your internal network configuration (a good idea to keep this information secure), provides automatic assignment of unregistered nonroutable IP addresses to internal clients, and provides a forwarding hand-off procedure for all requests for external services. Basically, Internet Connection Sharing transforms your Windows 2000 system into a limited DHCP proxy server. Try Hands-on Project 9-6 to configure Internet Connection Sharing.

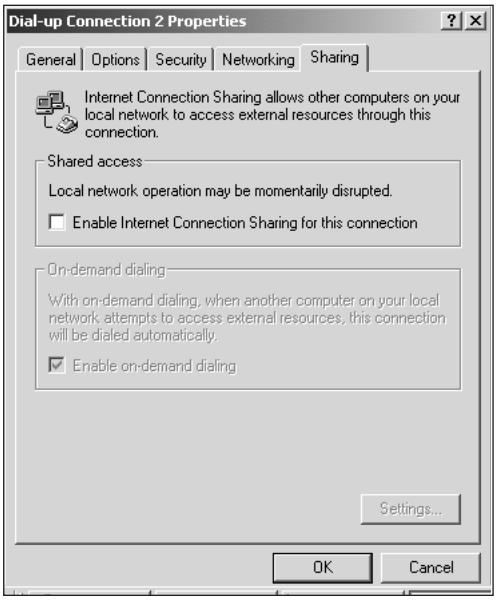


**Figure 9-10** The Properties dialog box for a private network connection object, Sharing tab

After Internet Connection Sharing is enabled, you can also select whether to enable on-demand dialing. This feature automatically reestablishes the remote link when a client attempts to access external resources over your system via the currently offline connection object. For further information about the tuning and configuration of the Internet Connection Sharing service, please consult the *Windows 2000 Resource Kit*.

Troubleshooting the Internet Connection Service involves three distinct activities. First, verify that the configuration options for Internet Connection Service are properly defined. This is done through the Settings button on the Sharing tab of a dial-up connection's Properties dialog box. Specifically, the settings for Internet Connection Service allow you to either custom define applications and TCP/UDP ports, or to select from a list of known common services such as FTP, IMAP, SMTP, POP3, and Telnet. Second, verify that the connection is active and functioning. This can usually be accomplished using a Web browser. Finally, verify that communication from other clients can access your system over the network by either PINGing or attempting to access a shared resource from your client.

## Dial-up to the Internet

The Internet has quickly become the communication medium of the masses. References to Web sites or e-mail addresses seem to be everywhere: on television, in magazines, in the local paper, and on thousands of products. Microsoft includes Internet access as a standard component of Windows 2000 remote communication. Windows 2000 also includes Internet Explorer and Outlook Express, in addition to the other common TCP/IP utilities often used over the Internet, such as File Transfer Protocol (FTP), Telnet, PING, and Tracert.

The Dial-up to the Internet Wizard can be used to establish a new user account with the MSN (Microsoft Network) dial-up network, move an existing MSN account to this computer, create a non-MSN Internet connection, or connect to the Internet over a network via a proxy server. A **proxy server** is software that sits between network users and the Internet, providing a layer of security to reduce the risk of network break-ins from the Internet. In most cases, you will either be configuring a non-MSN Internet connection or accessing a proxy server; however, if you want to employ MSN as your ISP (for an additional fee), simply select that option when prompted. To create a connection object for Internet access, follow the steps described in Hands-on Project 9-2.



After you have set up your connection object, if your modem is properly configured, your phone line is attached, and the service is not giving you a busy signal, you should have established an Internet connection, and the default homepage should be displayed in Internet Explorer. Close Internet Explorer by selecting Close from the File menu. You may be prompted to terminate your connection, but choose No to keep the connection active for now. Notice the connection icon in your icon tray—it is the one with the two overlapping monitors that blink. Double-clicking this icon opens the Connection Status dialog box (see Figure 9-11). You can terminate your connection at any time by clicking the Disconnect button in this dialog box.

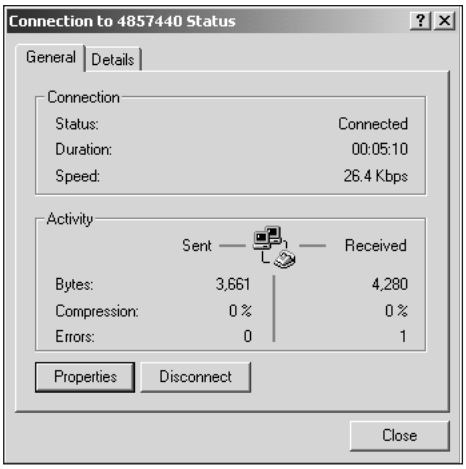


**Figure 9-11** The Connection status dialog box

If you selected the option to employ a proxy server to gain secure Internet access over a LAN, you will not see a connection object in the Network and Dial-up Connections window. Proxy connections are defined via the Internet Options applet (or by selecting the Internet Options command from the Tools menu of Internet Explorer), on the Connection tab, LAN Settings button. Any changes to your proxy settings should be made through the LAN Settings dialog box because a connection object is not created for proxy connections. Also, when you are employing a proxy connection over a LAN, the connection status icon does not appear in the icon tray.

The Connection Status dialog box is the same dialog box that appears for all dial-up connections. The General tab displays connection status, duration, speed, packets, compression, and errors. From this tab, you can access the connection object's properties or disconnect the link. The Details tab lists data such as server type, protocols, and the IP address of server and client.

The Properties dialog box of an Internet connection object is identical to that of a dial-up connection object. The only difference between these two objects is that one focuses on connecting to Windows 2000/Windows NT RAS servers and the other connects to ISPs.

## Connect to a Private Network Through the Internet

The VPN is a trend in mobile computing that employs the Internet as a long-distance carrier to enable distant secure LAN connections. The "Connect to a private network through the Internet" option of the connection wizard enables mobile or remote computers to establish a connection with a LAN over a local connection to an ISP. In other words, you can connect to the Internet anywhere in the world via a local access point, then use Windows 2000 VPN technology to link to your LAN. Such a RAS link offers you all of the functionality of a network client—except that the speed of the connection may not be as fast, depending on the communications link used. Furthermore, a Windows 2000 VPN encrypts not only your authentication credentials, but also all of the data transferred, ensuring private, secure, confidential, long-distance computing. To create a VPN connection object, follow the steps described in Hands-on Project 9-3.

After you have created a VPN connection object, the connection launch dialog box for it is displayed. Provide your logon name and password, and then click Connect to test the connection. If all settings are correct, you will have a VPN connection to your RAS server.

The RAS server to which you are connecting must be preconfigured to accept VPN connections. See the "Accept Incoming Connections" section to learn how to configure a Windows 2000 system to accept inbound connections.

The Properties dialog box for a VPN connection object is very similar to that of a dial-up connection object. The only differences are on the General and Networking tabs. The General tab (see Figure 9-12) offers control over the IP address/domain name of the RAS server and whether or not to employ a dial-up connection object to establish Internet access. The Network tab offers a pull-down list to select Automatic (selects a protocol already in

use automatically), PPTP, or L2TP connection types. This selection should be made on the basis of the setting of the RAS server to which you are connecting.

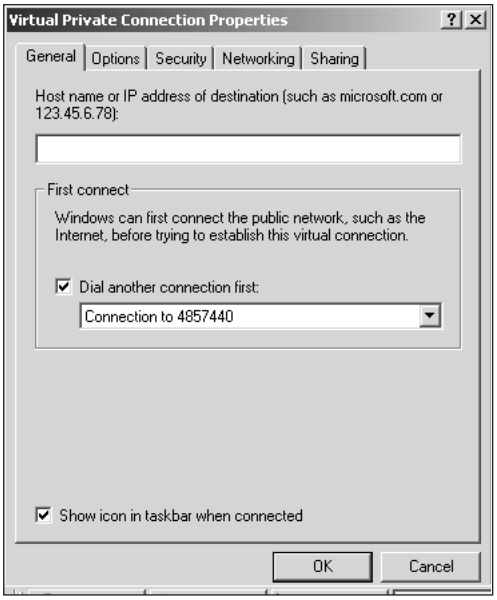


**Figure 9-12** The General tab of a VPN Connection object's Properties dialog box

## Accept Incoming Connections

Windows 2000 Professional, although designed as a network client, can act as a RAS server for a single inbound connection, which can occur over a modem, an existing Internet/network connection, or a direct access cable. You would probably use this feature only for special-purpose applications, for example, to gain access to your home system while traveling or to simplify technical support help for telecommuters. To configure Windows 2000 to accept an inbound connection, follow the steps described in Hands-on Project 9-4.

First, the incoming connection object is added to the Network and Dial-up Connection window, using the Make New Connection Wizard, as detailed in Hands-on Project 9-4. Opening this object's Properties reveals a dialog box with three tabs. The General tab (see Figure 9-13) is used to change the devices for this object and enable VPN connections. The Users tab is used to select which users can connect to this system over the inbound connection object. Furthermore, you can require that all users have "Require data encryption (disconnect if none)" set on their clients to protect passwords and data and decide whether to allow directly connected devices to connect without providing a password. By opening the Properties for a user, you can change that user's full name and password as well as set the callback options for that user. The Networking tab is where the networking components are configured.

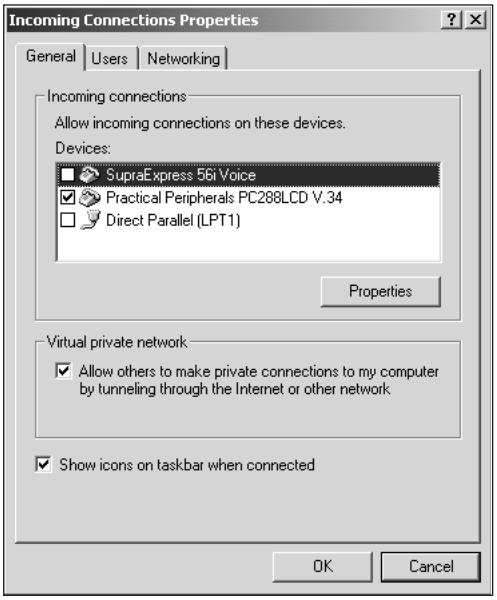


**Figure 9-13** The General tab of the Incoming Connections Properties dialog box

Once an incoming connection object is created, the devices selected for that object are placed into answer mode. Therefore, when a call is received by that device, Windows 2000 automatically answers the call and attempts to authenticate the connection. When a device is placed into answer mode, it can only be used by a single process for inbound connections. However, a device in answer mode can be used to establish outbound calls. In other words, creating an incoming connection object for your modem does not prevent you from using that modem to establish a connection with your ISP or office LAN. However, it does prevent you from running two answering processes at the same time, for example, RAS and a fax service.

## Connect Directly to Another Computer

All too often, you discover that you need to move several megabytes of data from one system to another, and either one or both of the systems do not have a network interface. In such cases, you have only a few reasonable options: use a tool that allows you to span copies across multiple floppy disks, purchase and install a NIC, or create a direct cable connection. Spanning floppies is often a doomed task, especially when working with more than 3 MB of material. If you do not have a NIC, the best option is to use a direct connect serial or parallel cable between the two computers, either connecting the COM ports or LPT ports (or even infrared ports, if already present on the systems), which you probably already have on hand or can purchase for less than $10.

To employ the direct connection, first attach the cable between the two systems, as mentioned either between COM or LPT ports (or orient the infrared devices). Next, you need to create a direct connection object on both systems—one acts as the host and the other acts

as the guest. Just be sure to select the correct link type based on your hardware (that is, serial, parallel, or infrared). To create the direct connection objects, follow the steps described in Hands-on Project 9-5.

You can create the host connection object through either the "Accept incoming connections" or the "Connect directly to another computer" wizard options. However, you can only create the guest or connect the object via the "Connect directly to another computer" wizard option.

After the link is established, you have a link to the other system just as if both systems were members of the same workgroup connected by network cables.

The Properties dialog box for a host direct connection object is the same as that of an incoming connection object. The Properties dialog box for a guest connection object is the same as that of any dial-up connection object, with the General tab offering control over the connection device.



## Installing RAS Hardware

Before any remote access connection can be established, the hardware required by that connection must be physically present and its drivers properly installed. Under Windows 2000, the process of installing hardware is often simple and requires little user input. Upon startup, Windows 2000 inspects the state of the hardware and attempts to identify any new devices. If a device's identity is recognized, it then attempts to locate and install drivers for that device. In some cases, you are prompted for additional paths to search for drivers. When Windows 2000 is unable to identify a device, you are either prompted to provide a path for the drivers or you need to use the Add/Remove Hardware applet or the Phone and Modem Options applet to install the drivers. For some specialty hardware, such as cable modems and DSL devices, you may need to use a vendor-supplied installation routine to install the correct drivers.

Because the range of RAS-related devices is so broad, we recommend consulting the device's manual or contacting the vendor for further help with installation. However, this should only be necessary for a few uncommon devices.

## Phone and Modem Options

The primary Control Panel applet related to remote access devices and operations is the Phone and Modem Options applet. This applet is used to control dialing rules, modems, and telephony driver properties. The Dialing Rules tab lists the defined dialing location. A dialing location is a collection of remote access properties used to govern how links are established. The Dialing Rules tab provides you with three buttons: New, which allows you to create new locations, Edit, to alter existing locations, and Delete, to remove a location. Both New

and Edit open the same three-tabbed interface in which the default or existing settings of a location can be altered.

The General tab of a new location (see Figure 9-14) is used to define:

- Location name
- Country/region
- Area code
- Number to dial to gain access to an outside line for local calls
- Number to dial to gain access to an outside line for long-distance calls
- Disable call waiting
- Dial using pulse or tone

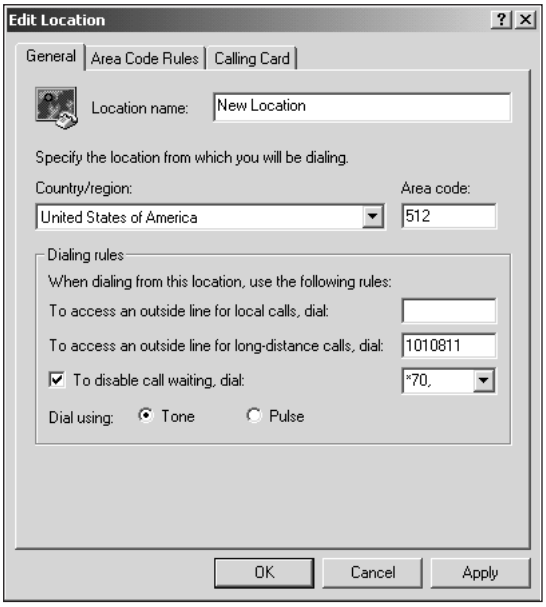


**Figure 9-14** General tab of a new location

The Area Code Rules tab is used to define how numbers are dialed that exist within the current area code or outside the current area code. These rules include which prefixes (the first three numbers of a seven-digit phone number) are included in an area code (and thus are local calls), whether to dial 1 first when calling certain prefixes, and whether to include the area code when dialing certain prefixes.

The Calling Card tab is used to define a method to charge long distance calls to a credit card or dialing card. There are dozens of predefined cards that only require you to provide your account number and PIN. In addition, you can define your own calling card billing rule. Please consult the online help and the *Windows 2000 Resource Kit* for details on calling card rule creation.

After you have created an alternate location (that is, set dialing rules), it will appear in a drop-down list on most connection interfaces. Therefore, each time you initiate a remote access link, you can select the location profile to use.

The Modems tab of the Phone and Modem Options applet lists all currently installed modems and their attached ports. New modems are installed by clicking the Add button, and existing modems are deleted using the Remove button. The Properties button is used to access device/driver-specific properties and configuration controls.

The Advanced tab of the Phone and Modem Options applet lists all of the telephony providers present on the system. These are the drivers employed by the remote access system to tie communications devices to the networking components. Telephony providers are the interface between the operating system and the communications device. In most cases, you never interact with this tab. Please consult the *Windows 2000 Resource Kit* or your telephone services provider for configuration information.

## WINDOWS 2000 AND THE INTERNET



Windows 2000 Professional provides a number of tools used in conjunction with the Internet: Internet Explorer, Outlook Express, FTP client, Telnet client, and Peer Web Services (PWS). The connections created via the Network and Dial-up Connections applet (such as a LAN with a proxy server) point to the Internet or to an Internet access and can be employed to access the vast resources of the Internet. Internet access is a key element in the design of Windows 2000. This is evident in ease of connecting to the Internet as well as the myriad tools included with the operating system.

### Internet Explorer

Microsoft Internet Explorer is included with the Windows 2000 operating system. Newer versions of (and updates to) Internet Explorer can be obtained from the Microsoft Web site at *http://www.microsoft.com/ie/*.

In a nutshell, Internet Explorer represents the best that a state-of-the-art Web browser can offer. In addition to being powerful and easy to use as a straightforward Web-surfing tool, Internet Explorer is tightly integrated with other Microsoft applications, so it can invoke Word to open .doc files or Excel to open .xls files across the Web. Internet Explorer also includes advanced support for newsgroups and FTP, and is tightly integrated with Outlook Express (a free version of Outlook 2000 available with Office 2000).

The latest release also includes support for Java and ActiveX controls, which can add powerful interactive features to Web pages. Finally, Internet Explorer includes built-in support for so-called "push" technologies (which allow you to send updated Web page information to registered customers automatically), and you have the option of choosing from numerous incoming channels of information (such as PointCast News, CNN, and other online information services) that can be piped into your browser on an ongoing basis.

## Outlook Express

One of the most popular e-mail client utilities is Microsoft Outlook, which is part of the suite of applications known as Office 2000. To tempt you with its impressive features and to offer you a taste of a multifunction e-mail client, Microsoft has included Outlook Express in Windows 2000. Outlook Express is limited only in the types of messaging it supports—specifically, it can only manage Internet e-mail involving POP3, IMAP, and SMTP services. Outlook Express can be used to read and write e-mail, file and sort messages, and more. It can act as a contact management tool, it is integrated with Internet Explorer for easy task switching, and it offers customizable interfaces and rules (actions to be performed on messages automatically).

If free is your highest criterion for an e-mail package, Outlook Express is no slouch. However, if you are willing to spend a few dollars for a worthwhile product, Outlook 2000 is worth the upgrade. For more information on Outlook 2000 and Outlook Express, please visit *http://www.microsoft.com/office/outlook/default.htm*.

## FTP Client

FTP is an IP-based protocol that handles file transfer and remote file system access and file manipulation functions. Microsoft includes a command-line implementation of an FTP client as part of the Windows 2000 operating system. This client is installed automatically when TCP/IP is installed.


To learn more about this program, launch a Command Prompt window (Start, Programs, Accessories, Command Prompt), then type *ftp* at the command line. When the ftp> prompt appears, type *help* to read the program's associated list of commands. (Type *help <command>* to obtain information about a specific command, and replace "*<command>*" with the name of an actual FTP command—for example, *get* or *put*.)

Even though the command-line version of FTP included with Windows 2000 is perfectly adequate, there are numerous freeware and shareware GUI implementations of FTP that are much easier and friendlier to use. For a complete listing of such utilities, visit either of the following Web sites, select Windows as the platform, and use "FTP" or "FTP client" as your search string:

- *www.shareware.com*
- *www.download.com*

## Telnet Client

Telnet is the text-based remote interaction tool commonly used on older UNIX systems to gain access to shell accounts (an account with an ISP that provides a text-only command-line interface to a remote system). Some ISPs still offer shell access to customers. The Telnet client included with Windows 2000 is a simple tool that attempts to establish a Telnet session with a remote system on the basis of domain name or IP address. You can alter the

display fonts and record the session for later perusal (remember, it's all text anyway). For more information on Telnet, enter *telnet* from a Command Prompt (Start, Programs, Accessories, Command Prompt), then type *?help* at the Microsoft Telnet prompt.

## Peer Web Services

Peer Web Services (PWS) is the Windows 2000 Professional version of Internet Information Services (IIS, a Windows 2000/Windows NT product). This application allows a Windows 2000 Professional system to host Web and FTP services. In most cases, PWS is used for site development and testing before deployment on an IIS system. PWS is limited to the same 10 simultaneous connections as Windows 2000 Professional itself; therefore, it is not a platform designed or intended for public Web/FTP site hosting. (Try Hands-on Project 9-7 to install PWS.)

Perhaps the most important, and in fact most widely recognized, function of PWS is the WWW (World Wide Web) Service, which allows users to publish Hypertext Markup Language (HTML) documents for use on the Web. Web browsers, such as Internet Explorer, use the Hypertext Transfer Protocol (HTTP) to retrieve HTML documents from servers.



Other than the limitation on the number of simultaneous users, and the omission of certain site management tools (such as FrontPage 2000, which is included with IIS 4.0, but not with PWS), the two environments are nearly identical. Certainly, they are more than consistent enough to facilitate development on Windows 2000 Professional and PWS, and deployment on Windows 2000 Server and IIS.

The FTP server installed with PWS is used to transfer files from the server to remote computers. Most installations of FTP on the Internet are used to download drivers and other data or software files.


The FTP Server code module represents the server side of FTP, whereas the FTP software mentioned earlier in the chapter deals with the client side of FTP. In other words, the FTP Server module allows other machines elsewhere on the network to upload files to a Windows 2000 Professional system, or to download files from that same system. The client-side software only allows the system to perform these activities with other FTP servers elsewhere on the network.

Web server resources are managed in much the same way as any other network resource. You should think of Web and FTP services as a type of share for Internet clients. Troubleshooting access problems for Web resources is performed in the same manner as dealing with the same issues regarding other network resource shares. Thus, you need to manage file permissions on an NTFS file object level and general access to resources via the share (or in this case Web or FTP services). If a user is unable to gain access to a resource via Web or FTP, first check the NTFS file object level permissions on the file/object/resource itself, then on all of its parent containers. Next, check the setting on the Web or FTP service. To access resources over the Web or FTP, the user must have at least Read access granted through the service, and at least Read access on the file or resource based on group memberships. Keep in mind that most Web access is anonymous, whereas most FTP access requires user authentication.

The anonymous user account, IUSR_<computername> is a member of both the Everyone and the Authenticated Users groups. So, be sure to check the permissions for these groups as well.

Try Hands-on Project 9-8 to practice managing resources hosted by a Web server. For more information on PWS, consult the *Windows 2000 Resource Kit*.

## Using Offline Files

One of the biggest problems with mobile computers is granting users access to important files and documents, whether they are connected to the office LAN or the Internet, or disconnected from all network mediums. Additionally, this problem is compounded by the hassle of managing file versions between the remote system and the office LAN or the Internet. To resolve this issue, Microsoft has developed a scheme known as Offline Files. Offline Files is a multipart solution that involves file designation, data transfer, and follow-up synchronization.

From a mobile system, you can enable access for files and folders on a case-by-case basis, even though a direct connection to the network is not established. Simply use My Network Places or Windows Explorer to view a list of shared folders or individual files. Right-click an item you want to be able to access while offline (or not directly connected to the network), then select "Make Available Offline" from the resulting menu. The selected items are transferred to a local storage area. When using this tool, the files and folders made available offline are still accessed in the same manner that they would be if they were not stored locally. Unlike the Briefcase from Windows NT, which makes a copy of the file and then requires you to access the copy via the briefcase container, Offline Files does not change your access methods and maintains the duplicate offline version of the files; all redirections are completely unseen by the user. The Windows 2000 method is much more elegant and logical than previous schemes. When you are not connected to the network, the browse lists of My Network Places and Windows Explorer list only those resources cached locally. When a file or folder is marked for offline access, its icon is altered to display a double-rotating-arrow overlay (you can see this folder symbol in Figure 9-15).

The first time a file is marked for offline availability, Windows 2000 launches a wizard that introduces you to the feature and helps with basic configuration. All of the settings offered through the wizard can be accessed at any time through the Offline Files tab (see Figure 9-15) of the Folder Options command from the Tools menu of Windows Explorer.

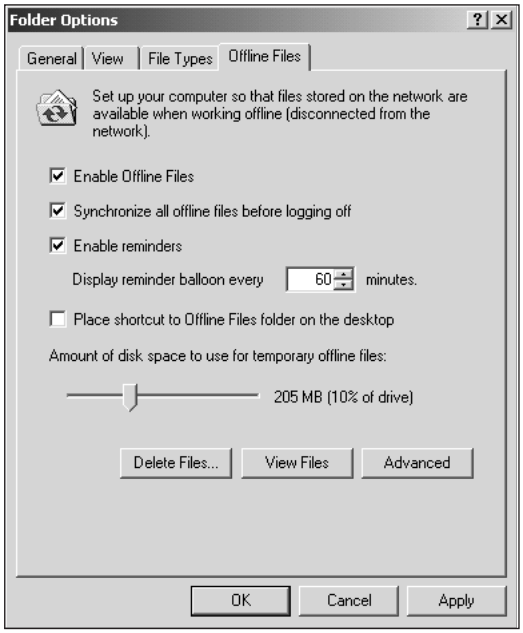


**Figure 9-15** Offline Files tab of the Folder Options command from the Tools menu of Windows Explorer

The controls on this tab are:

- Enable Offline Files
- Synchronize all offline files before logging off
- Enable reminders (to ensure that you are aware that you are working offline, displayed initially and then at defined intervals)
- Place shortcut to Offline Files folder on the desktop
- Amount of disk space to use for temporary offline files (this is a slider)
- Delete Files button
- View Files button
- Advanced button (determines how to deal with computers that go offline)

When the mobile system is reconnected to the network, Windows 2000 automatically synchronizes the offline files with their LAN-based originals. To alter the default, access the Synchronize Files command from the Tools menu of Windows Explorer. This interface lists all offline folders and their last updated status. To disable synchronization, deselect the check box beside a file or folder. To configure more advanced options, click the Setup button. Through this interface, you can define whether objects are synchronized automatically upon logon or logoff, only when idle, or at scheduled times.

Try Hands-on Project 9-9 to create and disable offline files. For more information on Offline Files, consult the *Windows 2000 Resource Kit*. File synchronization is also discussed in Chapter 15.

## REMOTE ACCESS TROUBLESHOOTING

Troubleshooting remote access problems can be fairly elusive; however, there are several common-sense steps and several useful Windows 2000 tools to simplify the process. Your first approach to a remote access problem should include checking the following:

- Physical connections, such as phone lines, serial cables, and so on
- Power to external devices
- Properly installed and updated drivers
- Properly configured settings
- Correct authentication credentials
- Similar encryption or security requirements
- Proper protocol requirements and settings

If reviewing these items still fails to uncover the problem, there are several log files you can examine to try to glean more specific information. There are three logs related to remote access events. The first log is a file containing all communications between the operating system and the modem device during connection establishment. This modem log must be enabled via the Diagnostics tab of the modem's Properties on the Modems tab of the Phone and Modem Options applet. Once enabled, a text file named after the modem (in the format "ModemLog_Practical Peripherals PC288LCD V.34.txt") is stored in the main Windows 2000 directory. This file can be viewed with Notepad or simply by clicking View Log next to the enable check box on the Diagnostics tab.

The second log file is the PPP.log file, which records the communications involved in the setup, management, and operation of a PPP connection. The easiest way to enable PPP logging is through the use of a Netsh command. At the command prompt enter the following to enable the PPP logging on the client:

**Netsh ras set tracing ppp enabled.**

This will cause the creation of a PPP.log in the **%**systemroot**%**\Tracing folder. You can then use any text editor to view the log file. If you wish to disable PPP logging on the client enter the following Netsh command at the command prompt:

**Netsh ras set tracing ppp disabled**.

(For more information on working with the Registry, see Chapter 13.)

The final log is the System log as viewed through the Event Viewer. This log often records events related to remote access connection failures. For more information about using logs and Event Viewer, see Chapter 11.

By combining the data gleaned from these logs, you should be able to determine the cause of your connection problem and easily discover a simple resolution. If you need further remote access troubleshooting help, consult the *Windows 2000 Resource Kit*.

## Chapter Summary

- Windows 2000 provides the Remote Access Service (RAS) to create remote WAN connections. This is done through support for various remote access and secure protocols.
- Windows 2000 simplifies the installation and configuration processes for RAS, and enables you to take full advantage of RAS dial-up networking and security features.
- The Internet access features built into Windows 2000 allow you to easily gain access to vast public and private resources.
- Windows 2000 is designed to participate in VPNs by establishing an encrypted link over the Internet between two systems.
- The Offline Files feature enables mobile computer users to work offline on files and folders used on the network.
- Finally, there are tools available to help you troubleshoot problems with RAS.



## Key Terms

**Dynamic Host Configuration Protocol (DHCP)** — A method of automatically assigning IP addresses to client computers on a network.

**gateway** — A computer that serves as a router, a format translator, or a security filter for an entire network.

**idle disconnect** — A feature that breaks off a RAS connection after a specified period of time has gone by with no activity. This feature reduces the costs of remote access, helps you troubleshoot by closing dead connections, and frees up inactive RAS ports.

**Integrated Services Digital Network (ISDN)** — A direct, digital, dial-up Public Switched Telephone Network (PSTN) Data Link layer connection that operates at 64 KB per channel over regular twisted-pair cable between a subscriber site and a PSTN central office.

**Internet Protocol Security (IPSec)** — A security protocol that secures data at the packet level.

**Layer 2 Tunneling Protocol (L2TP)** — A VPN (virtual private network) protocol developed by Cisco to improve security over Internet links by integrating with IPSec (IP Security).

**Multilink PPP** — The ability of RAS to aggregate multiple data streams into one network connection for the purpose of using more than one modem or ISDN channel in a single connection.

**NetBIOS gateway** — A service provided by RAS that allows NetBIOS requests to be forwarded independently of transport protocol. For example, NetBEUI can be sent over the network via NWLink.

**Point-to-Point Protocol (PPP)** — A Network layer transport protocol that provides connectivity over serial or modem lines. PPP can negotiate any transport protocol used by both systems involved in the link and can automatically assign IP, DNS, and gateway addresses when used with TCP/IP.

**Point-to-Point Tunneling Protocol (PPTP)** — A network protocol that allows users to create secure connections to corporate networks over the Internet, using virtual private networks (VPNs), which use encryption to transport private data across public links.

**port** — Any physical communications channel to which a modem, direct cable, or other device can be connected to enable a link between two computers.

**proxy server** — Software that sits between network users and the Internet, providing a layer of security to reduce the risk of network break-ins from the Internet.

**restartable file copy** — A RAS feature that automatically retransmits file transfers that are incomplete because of a RAS connectivity interruption.

**Remote Access Service (RAS)** — The service in Windows 2000 that allows users to log on to the system remotely over phone lines.

**Serial Line Internet Protocol (SLIP)** — An implementation of the IP protocol over serial lines. SLIP has been made obsolete by PPP.

**Telephony Application Programming Interface (TAPI)** — A Windows feature that supplies a uniform way of accessing fax, data, and voice. TAPI is part of the Windows Open System Architecture (WOSA) developed to aid third-party vendors in designing powerful, integrated telephony applications.

**virtual private networks (VPNs)** — Network connections that use encryption to transport private data across public links.

## Review Questions

1. You have configured a Windows 2000 Professional client to dial up and establish a connection to a Windows 2000 Server computer. The user adds a dial-up connection object and sets the proper network configuration, and the modem is functioning properly. The user submits the username and password correctly. Unfortunately, the user is unable to be authenticated properly. What might be causing this problem?
   a. The user did not configure the NetBIOS gateway properly.
   b. The user was not granted the appropriate dial-in permissions.
   c. The user was not added to the dial-in users group.
   d. none of the above
2. DHCP is the option for automatically assigning IP configurations to TCP/IP dial-up clients. True or False?
3. Windows 2000 Professional supports PPP logon scripts. True or False?
4. Which of the following RAS-related logs are enabled by default?
   a. PPP.LOG
   b. Modemlog_<*modem name*>.txt
   c. System log

5. Windows 2000 Professional supports which of the following encrypted authentication options through RAS? (Choose all that apply.)
   a. PAP
   b. SPAP
   c. DES-3
   d. MS-CHAP
6. The special protocol _____ allows multiple channels to be aggregated to increase bandwidth.
   a. Multilink PPP
   b. PPTP
   c. PPP
   d. SLIP
7. Where in Windows 2000 Professional do you specify which users have dial-in permissions to the RAS server?
   a. Network and Dial-up Connections
   b. Control Panel
   c. Remote Access Admin Tool
   d. My Computer
8. Which RAS security option also has an additional option to encrypt data?
   a. Require encrypted authentication
   b. Require C2 encrypted authentication
   c. Require B encrypted authentication
   d. Require Microsoft encrypted authentication
9. Which RAS callback option provides the greatest level of security?
   a. Set by caller
   b. Set by server
   c. Preset to
   d. Callback and confirm RAS password
10. Which of the following protocols are supported by both Windows 2000 RAS clients and RAS servers?
    a. SLIP
    b. PPP
    c. none of the above
    d. all of the above

11. Which of the following are similar technologies used to establish secured WAN links over the Internet? (Choose all that apply.)
    a. MPPP
    b. PPTP
    c. SLIP
    d. L2TP
12. Which LAN protocols are supported by RAS? (Choose all that apply.)
    a. AppleTalk
    b. TCP/IP
    c. NetBEUI
    d. DLC
    e. IPX
13. Which connection protocol can be used by Windows 2000 Professional to connect to remote systems over standard telephone lines?
    a. SLIP
    b. PPP
    c. DLC
    d. PPTP
14. Which connection protocol is retained by Windows 2000 to provide backward-compatibility with earlier versions of Windows NT, Windows for Workgroups, and LAN Manager?
    a. SLIP
    b. NetBIOS Gateway
    c. DLC
    d. AppleTalk
15. The Make New Connection Wizard from Network and Dial-Up Connections is used to create both RAS connections and LAN connections. True or False?
16. If you only want to connect to servers that offer secured data transmission, which of the following encryption settings should you define for your connection object?
    a. No encryption allowed (server will disconnect if it requires encryption)
    b. Optional encryption (connect even if no encryption)
    c. Require encryption (disconnect if sever declines)

17. Windows 2000 supports direct cable connections under RAS using which of the following? (Choose all that apply.)
    a. RS-232 null modem cables
    b. APC UPS cables
    c. LapLink cables
    d. Printer cables
18. RAS is remote control for Windows 2000. True or False?
19. Which two options from the Make New Connection Wizard are essentially the same, although one is used for calling an ISP whereas the other is used to call a RAS server?
    a. Dial-up to Private Network
    b. Dial-up to the Internet
    c. Connect to a Private Network Through the Internet
    d. Accept Incoming Connections
    e. Connect Directly to Another Computer
20. You can connect to another computer from a RAS client, using resources in the same manner as if you were connected on a LAN. True or False?
21. Dialing rules or dialing locations are used to define the geographic location of a mobile computer so as to prescribe the dialing procedures. True or False?
22. The modem-specific log file is enabled via which utility?
    a. Computer Management
    b. Phone and Modem Options
    c. Network and Dial-up Connections
    d. Server applet
23. Which of the following are Internet utilities included with Windows 2000 Professional? (Choose all that apply.)
    a. Internet Explorer
    b. Internet Information Server
    c. Outlook
    d. Telnet
    e. FTP client
24. The Offline Files mechanism of Windows 2000 is exactly the same as the Briefcase from Windows NT. True or False?
25. Offline Files are cached locally at logoff, are accessed in the same way as the original files, and are automatically synchronized by default. True or False?

## HANDS-ON PROJECTS


### Project 9-1

**To create a "Dial-up to Private Network" connection object:**


This hands-on project assumes that a modem is installed.

1. Launch the Make New Connection Wizard by double-clicking the **Make New Connection** icon displayed in the Network and Dial-up Connections window.
2. The first page of the wizard is a welcome message. Click **Next**.
3. Select the network connection type to create, select **Dial-up to private network**, then click **Next**.
4. Provide the dial-up number for your RAS server.
5. If this RAS client is a mobile computer (notebook, portable, etc.), select the **Use dialing rules** check box, then provide the area code, and select the country/region code.
6. Click **Next**.
7. Set the availability of this connection. Your options are to allow all users of this system access to this connection object or to restrict access to your user account.
8. Click **Next**.
9. Finally, define a name for this connection. The default Dial-up Connection name can be changed to something descriptive, such as the name of the RAS server or the network this object will be used to connect to.
10. If you want this object to appear as a shortcut on the desktop, select the **Add a shortcut to desktop** check box.
11. Click **Finish**.
12. The Make New Connection Wizard completes the connection object creation (that is, it now appears in the Network and Dial-up Connections window); however, instead of returning to the Network and Dial-up Connections window, the new connection object is launched for the first time.
13. The Connect dialog box (see Figure 9-16) displays connection details for this connection object.

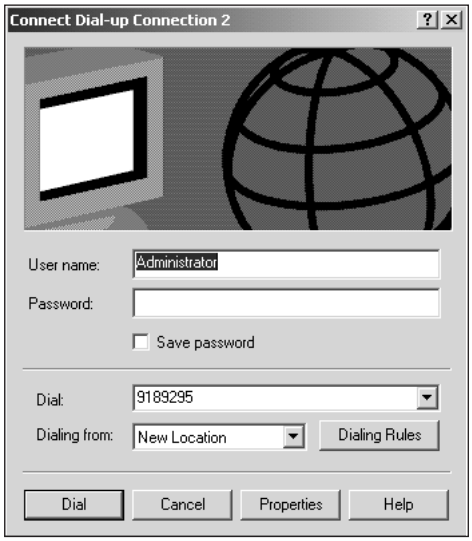


**Figure 9-16** The Connect dialog box for the newly created Dial-up to private network connection object



14. In the User name field, type the name of the user account you need to employ when connecting to the remote RAS system.
15. In the Password field, type the password for that user account—your keystrokes are echoed with asterisks instead of the actual character you type to prevent over-the-shoulder theft of your password.
16. If you want the system to retain your password, select the **Save password** check box. If you decide not to check this box, you will have to provide the password each time this connection object is used to establish the RAS link.
17. Double-check that the listed phone number in the Dial field is correct. If not, change it to the correct number.
18. If you are working from a mobile system, select the dialing location in the Dialing from field. If your current location is not predefined, click **Dialing Rules** to create a new location profile.


## Project 9-2

**To create a Dial-up to the Internet connection object:**


This hands-on project assumes that a modem is installed.

1. Launch the Make New Connection Wizard by double-clicking the **Make New Connection** icon displayed in the Network and Dial-up Connection window.

2. The first page of the wizard is a welcome message. Click **Next**.
3. Select the network connection type to create, select **Dial-up to the Internet**, then click **Next**.
4. This launches the Internet Connection Wizard, which prompts you for the type of Internet connection. Your choices are to create a new MSN account, move an existing MSN account, or connect to a non-MSN ISP/network proxy. For our purposes, select the final option that states **I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)**. See Figure 9-17. Then, click **Next**.

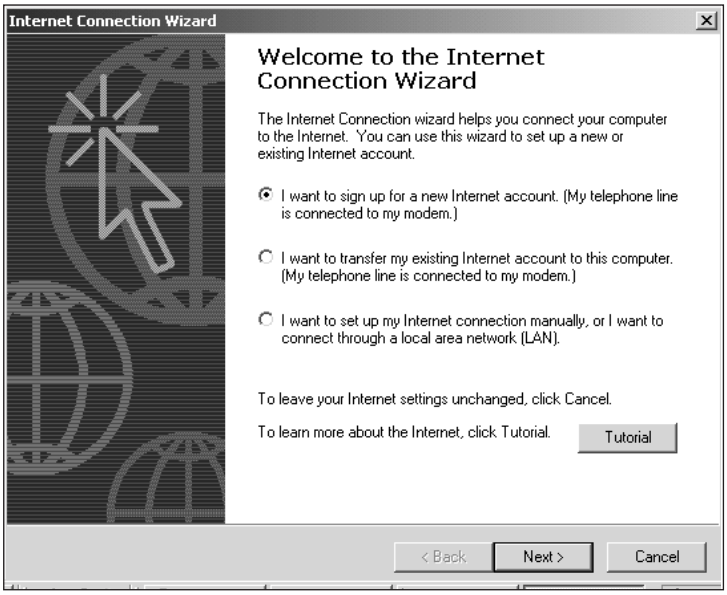


**Figure 9-17** The Internet Connection Wizard

5. Next, indicate which type of connection you want to establish. The choices are a modem connection or over a LAN. If you are using a modem, select that radio button. If you are using a LAN connection, select that radio button. Modem users click **Next**, then continue to Step 6. LAN users click **Next**, then jump to Step 16.
6. Select the dialing device from the pull-down list of installed modems. Click **Next**.


If there is only one modem or dialog device installed, you will not see the wizard screen in Step 6.

7. Provide the telephone number for the ISP. Verify that the area code and country/region settings are accurate.

8. If your ISP requires advanced settings (most do not), click the **Advanced** button. This reveals a dialog box in which you can select the connection type (PPP, SLIP, or CSLIP), logon procedures (none, manual logon, or logon script), IP address (automatically assigned or static), and DNS server address (automatically provides or primary/alternative static defined). All of these settings can be altered via the properties for this connection object after its initial creation.
9. Click **Next**.
10. Provide the username and password used to log on to the ISP. Click **Next**.
11. Provide a name for this connection object. Click **Next**.
12. Next the Wizard asks if you wish to configure Outlook Express to retrieve your e-mail, if so select **Yes**; otherwise, select **No**. Click **Next**.
13. If you selected **Yes**; you must provide a profile name, the e-mail address, the POP3, IMAP, or HTTP server address for incoming mail, the SMTP server address for outbound mail, and mail system authentication credentials (username and password). Provide the data required and click **Next** to proceed through the E-mail Setup Wizard.
14. The final page of the Internet Connection Wizard has a check box stating: To connect to the Internet immediately, select this box then click Finish. Follow those instructions. This completes the creation of the connection object. The system launches Internet Explorer, attempts to establish an Internet link using the newly created connection object, then loads the MSN homepage.
15. If you are a modem user, skip the remainder of these steps.
16. If you are using a LAN to gain Internet access, you are prompted for the method to obtain proxy configuration information. You can select **Automatic** or provide the URL of the configuration script. Your proxy server documentation informs you of which method to employ. Make a selection, provide the URL if necessary, then click **Next**.
17. If you want to configure Outlook Express, select **Yes**, otherwise select **No**. Click **Next**. Review Step 13 if you selected Yes.
18. The final page of the Internet Connection Wizard has a check box stating: To connect to the Internet immediately, select this box then click Finish. Follow those instructions. This completes the creation of the connection object. The system launches Internet Explorer, attempts to establish an Internet link using the newly created connection object, then loads the MSN homepage.


## Project 9-3

**To create a Connect to a Private Network Through the Internet connection object:**

1. Launch the Make New Connection Wizard by double-clicking the **Make New Connection** icon displayed in the Network and Dial-up Connections window.
2. The first page of the wizard is a welcome message. Click **Next**.
3. Select the network connection type to create, select **Connect to a private network through the Internet**, then click **Next**.

4. The **Network Connection Wizard** prompts you for whether this object will automatically dial an existing ISP connection object or will rely upon you to establish a connection manually before launching this VPN connection object. If you change locations often and require unique access point phone numbers, selecting manual connection is your best choice. However, if you reuse the same access point often, allowing the VPN connection object to make the connection automatically simplifies your connection activities. For now, select automatic and select the ISP connection created previously. Click **Next**.
5. Provide the IP address or fully qualified domain name (FQDN) of the RAS server you want to connect to over the Internet. Click **Next**.
6. Indicate whether this VPN connection object will be available to all users or only to you. Click **Next**.
7. Provide a name for this connection object, then indicate whether to create a desktop icon. Click **Finish**.


## Project 9-4

**To create an Accept Incoming Connections connection object:**

1. Launch the Make New Connection Wizard by double-clicking the **Make New Connection** icon displayed in the Network and Dial-up Connections window.
2. The first page of the wizard is a welcome message, click **Next**.
3. Select the network connection type to create, select **Accept incoming connections**, then click **Next**.
4. The Network Connection Wizard prompts you for the device over which a connection will be answered. This should list all modems and access ports (serial, parallel, and infrared). Mark the check boxes beside one or more devices.
5. If you need to alter the settings of a device, select it from the list, then click **Properties**. This reveals a device-specific settings dialog box.
6. Click **Next**.
7. Select whether to allow VPN connections. (VPN connections require a static IP address.) Click **Next**.
8. Select which users can establish a VPN connection with this system. Mark the check box beside each user to allow them to connect. You can create new users by clicking the **Add** button. Click **Next**.
9. The wizard offers you the ability to configure or alter the networking components to be used over this link. This interface is the same as the one seen when configuring other connection objects, and lists the protocols, services, and clients currently installed. Make any necessary changes, then click **Next**.
10. Provide a name for this Incoming connection. Click **Finish**.


## Project 9-5

**To create a Connect Directly to Another Computer connection object:**

1. Go to the system that will act as the host in the direct connect pair. Typically, the host system has the resource that needs to be transferred or accessed by the guest system.
2. Launch the Make New Connection Wizard by double-clicking the **Make New Connection** icon displayed in the Network and Dial-up Connections window.
3. The first page of the wizard is a welcome message, click **Next**.
4. Select the network connection type to create, **Connect Directly to Another Computer**, then click **Next**.
5. Select the **Host** option. Click **Next**.
6. Select the link device type (serial, parallel, infrared, etc.) from the drop-down list. Click **Next**.
7. Select the user(s) who can connect over this link. Click **Next**.
8. Provide a name for this connection object. Click **Finish**.
9. Go to the system that will act as the guest in the direct connect pair.
10. Launch the Make New Connection Wizard by double-clicking the **Make New Connection** icon displayed in the Network and Dial-up Connections window.
11. The first page of the wizard is a welcome message. Click **Next**.
12. Select the network connection type to create, **Connect Directly to Another Computer**, then click **Next**.
13. Select the **Guest** option. Click **Next**.
14. Select the link device type (serial, parallel, infrared, etc.) from the drop-down list. Click **Next**.
15. Select the option to restrict this object to the current user or to allow all users access. Click **Next**.
16. Provide a name for this connection object. Click **Finish**.
17. The **Connect Direct Connection** dialog box appears. Provide a name and password (for a user account granted access to connect in Step 7). Click **Connect**.


## Project 9-6

**To configure Internet Connection Sharing:**


This hands-on project requires that a dial-up connection already be defined.

1. Open the Network and Dial-Up Connections tool by selecting **Start**, **Settings**, **Network and Dial-Up Connections**.

2. Select the predefined dial-up connection item from the Network and Dial-Up Connections tool.
3. Select **Properties** from the **File** menu.
4. Select the **Sharing** tab.
5. Select the **Enable Internet Connection Sharing for this connection** check box.
6. Click the **Settings** button.
7. Select the **Services** tab.
8. Select the checkbox beside **FTP Server**.
9. Click **OK**.
10. Click **OK**.


## Project 9-7

**To Install Peer Web Services on a Windows 2000 Professional system:**

1. Open the Control Panel by selecting **Start**, **Settings**, **Control Panel**.
2. Double-click the **Add/Remove Programs** icon.
3. Select the **Add/Remove Windows Components** item in the left column. This launches the Windows Component Wizard.
4. Select the check box beside **Internet Information Services (IIS)**.
5. Click **Next**.
6. When prompted, provide the path to the Windows 2000 Professional CD. This may involve just inserting the CD into the drive and clicking OK, or using a Browser dialog box to locate the \i386 directory on the CD.
7. The installation wizard will copy files to your system. This will take several minutes. You may be prompted for the path to the CD a second time. Eventually, click **Finish**.
8. Click **Close** to terminate the Add/Remove Programs applet.
9. Close the Control Panel by selecting **Close** from the **File** menu.


## Project 9-8

**To manage resources hosted by a Web server:**

1. Launch the Personal Web Manager from the Administrators. Tools applet in the Control Panel by selecting **Start**, **Settings**, **Control Panel**. Double-click **Administrative Tools**, then double-click **Personal Web Manager**.
2. On the Main page, which appears by default, take note of the path for **Your home directory**.
3. Select **Exit** from the **Properties** menu in the Personal Web Manager.
4. Launch Windows Explorer by selecting **Start**, **Programs**, **Accessories**, **Windows Explorer**.

5. Locate the folder as indicated by the path on the Main page of the Personal Web Manager and select it in the left pane of Windows Explorer.
6. In the right pane of Windows Explorer, right-click over an empty area, select **New** from the pop-up menu, then select **Text Document** from the resulting menu.
7. Type **default.htm** as the filename, then press **Enter**. If prompted about whether to change the filename extension, click **Yes**.
8. Open Notepad by selecting **Start**, **Programs**, **Accessories**, **Notepad**.
9. Select **Open** from the **File** menu.
10. Change the **Files of type** pull-down list to **All Files**.
11. Locate and select the **default.htm** document.
12. Click **Open**.
13. Type the following into the body of this document: **<HTML><BODY>This is the default document.<P></BODY></HTML>**.
14. Select **Save** from the **File** menu.
15. Select **Exit** from the **File** menu.
16. Double-click the **Internet Explorer** icon on the desktop.
17. Select the **Open** command from the **File** menu.
18. Type **localhost** and click **OK**.
19. The Web browser should display the default document you created by showing a line stating **This is the default document**.
20. Select **Close** from the **File** menu of Internet Explorer.




## Project 9-9

**To create and disable offline files:**


This hands-on project requires that Windows 2000 Professional be a client in a Windows network and that some online resources are available via a share.

1. Open Windows Explorer selecting **Start**, **Programs**, **Accessories**, **Windows Explorer**.
2. Expand the **My Network Places** area of Windows Explorer, then expand **Entire Network** and expand **Microsoft Windows Network**.
3. Locate and select a share on any accessible network host.
4. Right-click over the selected share and select **Make Available Offline** from the pop-up menu. This launches the Offline Files Wizard.
5. Click **Next**.

6. Verify that the **Automatically synchronize the Offline Files when I log on and log off my computer** checkbox is selected. Click **Next**.
7. Verify that the **Enable reminders** checkbox is selected and the **Create a shortcut to the Offline Files folder on my desktop** checkbox is not selected. Click **Next**.
8. Select **Yes, make this folder and all its subfolders available offline**, then click **OK**.
9. After the synchronization process, all files that are stored as Offline Files will have a small double arrow image added to their icon to identify it. To disable Offline File support, select an enabled folder, right-click, and select **Make Available Offline**. This will remove the checkbox beside this command and remove the files from local cached storage.

## CASE PROJECTS


1. Your organization has decided to allow several employees to work from home. With Windows 2000 Professional on the telecommuters' systems, describe your configuration and setup options, including how you can deal with security and nondedicated connections.
2. After installing a new modem, none of your connection objects will function—even after you've re-created them. Describe the process you would use to troubleshoot this problem.